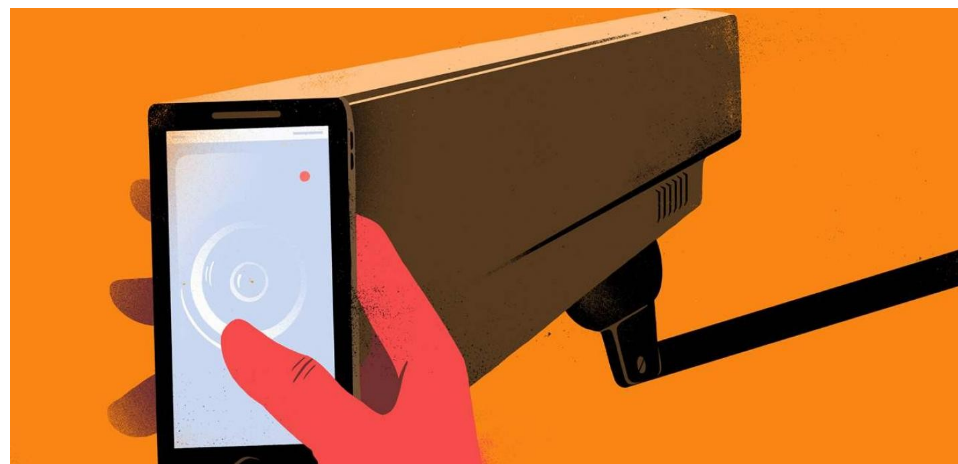
Cette brochure a pour envie de recenser des problématiques liées à la surveillance policière des téléphones, et de donner des petites astuces pour réduire les risques liés à cela.

Il s'agit ici de la seconde version de cette brochure. Elle comporte des erreurs, raccourcis, incertitudes – de plus tout ce qui est attrait au numérique évolue vite. N'hésite pas à en faire des critiques pour faire évoluer ce texte, au contact :

autodefense-numerique@riseup.net

Téléphonie mobile

Surveillances, répressions, réduction des risques



Seconde version : mai 2025

Table des matières

Introduction....3
I) La téléphonie mobile et la sécurité....4
Les réseaux d’antennes téléphoniques []....4
Les enjeux spécifiques pour les téléphones portables....5
Le système d’exploitation du smartphone....7
II) Les problèmes inévitables de sécurité dans les téléphones []....9
Géolocalisation du téléphone []....9
Appels et SMS en clair []....9
Identification des téléphones []....10
Failles de sécurité et mises à jour....12
Données de la carte sim et du téléphone []....13
Communiquer c’est à plusieurs []....13
III) Outils des keufs....14
Interceptions administratives et judiciaires []....14
En garde à vue / audience / instruction / enquête....15
Le Kiosk – extracteur de téléphone....16
IMSI-catcher – les fausses antennes relais []....17
Perquisition à domicile []....18
Boites noires....18
Équipes technologiques de la police []....18
Exploitation de failles de sécurité....20
Analyst's Notebook et logiciels d’analyse de données []....20
Tentative de restauration des données à partir d’appareils endommagés []....21
Installation de mouchards (matériel ou logiciel) []....21
IV) Réduction des risques....23
1) Habitudes []....23
2) Applis libres....24
Revenons sur Signal....30
Avoir signal sur ordinateur....32
Utiliser Signal sans Signal....32
3) Paramètres du smartphone....33
4) Avoir un téléphone dont la carte SIM est « anonyme » []....35
5) Changer de système d'exploitation:....36
5) Trucs techniques avancés / divers pour smartphone....36
Lexique....38
Ressources supplémentaires....38

Lexique

Logiciel libre vs logiciel propriétaire
Avant de continuer il est important de comprendre la différence.
Un **logiciel libre** ou **open source**, sont des logiciels dont on a accès au code source, c'est à dire dont on peut avoir accès à la recette du logiciel pour savoir comment il fonctionne (le logiciel libre va plus loin car il offre la liberté de modifier, redistribuer, modifier le logiciel en plus d'avoir accès à la recette).
Le **logiciel propriétaire** n'offre pas l'accès au code source. Cela signifie qu'il ne peut pas y avoir d'avis extérieur à la structure qui fourni le logiciel propriétaire, on remet 100 % de notre confiance à l'entreprise qui a créé le logiciel en terme de sécurité et de respect de nos données personnelles.
Information en claire vs information chiffrée
Une information est dite en « **claire** » si toute personne / machine qui y a accès peut avoir accès au contenu directement.
Elle est dite **chiffrée**, s'il existe un langage (en numérique un algorithme mathématique) rendant impossible (ou compliqué) d'accès au contenu aux personnes / machines qui ne connaisse pas l'algorithme pour le déchiffrer. Il existe plusieurs technologies / langage pour faire du chiffrement, dont les qualités varient énormément.

Fork : C'est un nouveau logiciel créé à partir du code source d'un logiciel existant. Son existence découle d'un choix politique venant de visions différentes du projet des différents acteurs qui y participent, un acteur décidant alors de créer cette *dérivation* pour lui imposer les idées qu'il n'a pas pu soumettre au précédent projet,
Métadonnées : Les métadonnées, c'est ce qui décrit le contexte autour de la donnée. Dans un sms il y a la donnée qui est le sms en tant que telle, la métadonnée c'est la taille du sms, qui écrit à qui, à quelle heure, etc.

Ressources supplémentaires

* Site internet de La quadrature du net sur l'évolution des lois numériques : https://laquadrature.net
* Surveillance Self-Défense (pas toujours traduit en français) : https://ssd.eff.org/
* Guide sur la sécurité des téléphones portables et sécurité des activistes (en anglais). Mobile phone security for activist and agitator
* Guide d'autodéfense numérique pour tout ce qui touche aux ordinateurs : https://guide.boum.org
* Listes logiciels libres alternatifs (logiciel libre ne veut pas dire sécurisé pour ce que tu veux faire) :
- https://technopolice.be/autodefense-numerique/
- https://www.chatons.org/
- https://riseup.net/fr/security/resources/radical-servers

Introduction

Ce texte a été fait principalement à partir d'un compte rendu de formation sur la question de téléphonie mobile, complété avec des bouts trouvés sur internet, car de manière générale on manque de ressources sur cette thématique dans les milieux militants. Certaines parties parlent des problématiques de surveillance policière liée à la téléphonie de manière générale (et sont symbolisées en début de chapitre par [📞] et dans la table des matières par []). Ces parties traitent les problématiques à la fois pour les téléphones à bouton et pour les smartphones. D'autres parties parlent plus des smartphones (📱). Les mots avec une * sont explicités dans un lexique à la fin de la brochure.

On trouve plus d'outils de réduction des risques pour les smartphones, mais on retrouve les mêmes problématiques qu'avec les téléphones à boutons, et les smartphones ont aussi d'autres problématiques en terme de sécurité. Parfois les outils offrent des sensations de sécurité qui font oublier leurs limites, et poussent à diffuser des informations sensibles qu'on aurait mieux fait de faire passer par d'autres canaux.

Si l'angle de ce document se porte sur les questions d'enjeux de surveillance et d'outils de sécurité vis-à-vis de la répression de L'État, on pourrait aborder ces problématiques par d'autres angles, que ce soit en usage collectif ou individuel :

- Écologie et colonialisme car il faut 70 matériaux différents et 70 kg de matière extraite et assemblée par des personnes sous-payées, dans des pays colonisés par le capitalisme pour construire un smartphone qui sera détruit rapidement[1]

- Résistance à la pression de passer toujours plus par ces outils, pour le travail ou les administrations, la banque, les démarches de santé et autres et qu'il y a souvent plein d'astuces à se transmettre pour ne pas avoir à fournir de numéro de téléphone ou pour pouvoir rester déconnecté·e

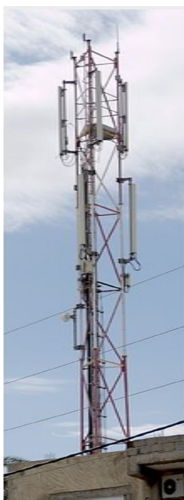
- Que ces outils sont aussi des sources d'exclusions pour les personnes qui n'y ont ou ne souhaitent pas y avoir accès, ou qui manquent de compétences. Il est important au sein des collectifs d'avoir des discussions à ces sujets pour que la sécurité ne deviennent pas un outil de domination pour certain.es.

- Défense de nos données contre les multinationales, même si certaines propositions se recoupent car les multinationales sont facilement sollicités par les flics[2].

1 Voir pour l'analyse le dossier par exemple de « L'emprunte cachée des smartphones » de France Nature Environnement, même si les positionnements politiques ne vont pas très loin.
2 2 exemples: la collaboration de Google, facebook, twitter et microsoft avec la commission européenne dans la lutte contre le terrorisme: https://www.laquadrature.net/2019/04/26/reglement-terroriste-premier-bilan-et-prochaines-etapes/, ceux ci ont leur propre liste de personnes ou contenu « terroriste ». Ou sur le site transparency de google, on peut lire autour de 20 000 requêtes judiciaires par an par la france, dont 80 % amènent à des données envoyés https://transparencyreport.google.com/user-data/overview.

I) La téléphonie mobile et la sécurité

Les réseaux d’antennes téléphoniques [📞]



Le portable se connecte par ondes électromagnétiques à des antennes / cellules. L’antenne reconnaît alors la validité de la carte SIM et du téléphone. La carte sim contient un numéro d’identification (IMSI) que l’opérateur vérifie afin d’autoriser ou non les communications avec d’autres téléphones.

Les antennes ne communiquent pas directement entre elles. Elles sont le lien entre le réseau de l’opérateur et les téléphones. Les communications sont transportées d’une antenne à l’autre par des câbles ou parfois avec d’autres ondes telles que la wifi. En plus de ces câbles et de ces ondes, nos communications passent par des ordinateurs (des routeurs et autres) qui acheminent le signal d’un endroit à un autre jusqu’à des nouvelles antennes et aux téléphones avec lesquels on communique.



Tout ce matériel réseau est possédé par des entreprises privés qui, comme toutes les boîtes, veulent se faire des sous ou avoir du pouvoir. Il n’est pas possible de faire confiance au matériel du réseau.

Les nouvelles technologies s’ajoutent aux anciennes, elles ne les remplacent pas. Les technologies GSM s’accumulent : en plus de la 4G et de la 5G (et d’ici peu de la 6G), il y a encore la 2G, 3G et d’autres, même s’il y a la volonté d’enlever la 2G un jour. Ces antennes sont présentes en ville, sur des immeubles, parfois cachées par des tissus, sinon plus généralement sur des pylônes.

Les opérateurs communiquent entre eux afin qu’on puisse s’appeler de chez orange à chez Lyca par exemple, et vice-versa. Les opérateurs ont aussi des contrats avec des fournisseurs d’internet, pour permettre l’accès internet sur les téléphones de leurs réseaux.

Un téléphone essaie toujours de se connecter à plusieurs antennes afin de permettre de garder la communication même lorsqu’on se déplace. Mais si on est dans une zone avec uniquement des antennes Free et qu’on est chez Bouygues, alors on captera pas. Quand on va dans un pays autre que celui où on a notre abonnement, on se connecte à des réseaux qui ont des contrats avec notre opérateur, ça s’appelle l’itinérance (ou le « roaming »).

Appli SnoopSnitch

Pour les téléphones android seulement : SnoopSnitch analyse le micrologiciel de votre téléphone à la recherche de correctifs de sécurité Android installés ou manquants. Pour les android « rooté » ce logiciel peut permettre de détecter les IMSI catcher.

- Gratter le numéro marqué sur la SIM (IMSI ou autre)

- Gratter celui ou ceux marqués sur le tél (IMEI, à l’intérieur)

- Installer un filtre de confidentialité. Il s’agit d’un film à mettre sur l’écran qui permet de rendre opaque ce qui se trouve sur l’écran quand on le regarde avec un angle de plus de 30°. Peut être intéressant pour l’usage du smartphone d’activités confidentielles dans un espace passant. Prix entre 10 et 20 euros en fonction des téléphones.

- Inviter à ce qu'il y ait plus de gens à utiliser ces techniques c'est se protéger dans la masse. Si dans une manif il n'y a qu'un téléphone d'une carte prépayée qui borne, il pourrait paraître suspect en cas d'enquête.

5) Changer de système d'exploitation:

⇒ Nécessite d'avoir un téléphone compatible (liste disponible sur les sites respectifs des systèmes d'exploitation)
⇒ Attention, ça ne résout pas les problèmes inévitables, et surtout libre ne signifie pas sécurisé face à la police !![23]
⇒ Système d'exploitation libre* existant : LineageOS[24], CalyxOS, GrapheneOS, CarbonROM, /e/, DivestOS Mobile[25], … La plupart sont très compliqués à installer / mettre en œuvre et doit être fait avec des personnes ayant des compétences avancées.

Se procurer un téléphone Pixel et installer GrapheneOS

GrapheneOS est un système d'exploitation mobile libre axé sur la sécurité et la confidentialité avec compatibilité avec les applications classiques Android. C'est le système d'exploitation le plus fiable en terme de sécurité numérique à ce jour et il est plutôt facile à installer. Cependant il n'est compatible qu'avec les téléphones Google Pixel (prendre les versions 6a ou plus récente, les anciennes versions on un soucis de sécurité[26]). Pour installer GrapheneOS sur son Pixel, le mode d'installation est bien plus accessible que les autres systèmes d'exploitation mobile, il faut suivre les instructions qu'il y a sur leur site (https://grapheneos.org/install/web), qui n'est disponible qu'en anglais.

Les informations du collectif technopolice belgique sur les systèmes d'exploitations téléphoniques en terme de sécurité, avec leur durée de développement en fonction du téléphone sont retrouvables ici : https://technopolice.be/smartphones/

5) Trucs techniques avancés / divers pour smartphone

Cette section est plus développé sur https://telmob.0id.org/fr:divers.
Ces trucs sont potentiellement pas hyper accessibles sans un peu de compétences techniques, d'acharnement, ou de moyens financiers. Si des collectifs de geek existent dans ton coin ça vaut le coup de leur demander conseils.

23 Pour des comparaisons de système d'exploitation de téléphone en terme de sécurité, voir ici (infos en anglais et technique): https://eylenburg.github.io/android_comparison.htm
24 Un très bon tutoriel explicatif de pourquoi et comment installer LineageOS sur smartphone est disponible à cette page : https://linuxfr.org/news/installer-lineageos-sur-son-appareil-android
25 Modèles de téléphones disponible: https://divestos.org/index.php?page=devices&base=LineageOS
26 Les versions avant Pixel 6 peuvent subir du brute force par le logiciel Cellebrite: https://next.ink/144397/tentative-dassassinat-de-trump-cellebrite-deverrouille-un-samsung-mais-peine-avec-apple-et-google/

Les enjeux spécifiques pour les téléphones portables

Les téléphones sont fabriqués par des grosses entreprises capitalistes. Le matériel fabriqué n'est pas libre*, on ne sait pas la liste exacte des composants et de comment ça marche. Il y a parfois quelques notices pour réparer des bouts, mais on ne peut jamais réparer le tout. En d'autres termes, la recette n'est pas fournie.

Pour les **téléphones à boutons** de manière générale il n'y a pas trop de sécurité possible à espérer dessus. Il existe des téléphones à boutons avec des systèmes d'exploitation permettant de les chiffrer ou d'utiliser quelques applications sécurisantes[3] (dans lesquelles il est malheureusement difficile voire impossible d'avoir confiance), dans ce cas on trouve les mêmes problématiques que les « téléphones intelligents ».



Vue éclatée d'un smartphone avec ses différents composants.

Les téléphones dits « intelligents » ou **smartphones** font ce pourquoi ils ont été fabriqués et rien de plus. Ils ne sont pas intelligents ! En réalité il s'agit du même outil qu'un téléphone à boutons : c'est un petit ordinateur. Seulement le smartphone est plus puissant et contient plein de capteurs : de quoi mesurer les vitesses de

3 On peut trouver des marques sur ce site internet : https://dumbphones.pory.app/

déplacement, d'accélération, le rythme cardiaque (ce capteur qui permet de calculer le rythme cardiaque est tellement puissant qu'il pourrait en théorie reconstituer le son à partir des vibrations même si le micro est fermé), la luminosité ambiante, caméras, gyroscope, magnétomètre, … De nombreux smartphones sont aussi puissants qu'un ordinateur milieu de gamme, voire plus.

Les téléphones ont des problématiques spécifiques de sécurité numérique :

- contrairement aux ordis ils sont [*pour la plupart des usager.es*] toujours allumés avec énormément de données dedans dont une partie qu'on n'a pas décidé d'avoir.
- Y a pas de normes matériels sur les téléphones portables. Les fabricants de téléphones [Samsung, Google, Apple, ….] achètent les différents composants (écran, gsm, carte wifi, batterie, …) et assemblent le tout. Dans les ordis il y a beaucoup plus de normalisation et de compatibilité des composants entre les différents ordis. Ces composants spécifiques à chaque modèle de téléphone rend plus compliqué d'avoir des systèmes d'exploitation alternatifs (plus sécurisés que celui installé à l'origine ou avec une idéologie moins douteuse, par exemple). Le matériel est fabriqué par des entreprises privées soumises aux États. Les téléphones sont fournis avec des logiciels propriétaires*, il y a peu de volonté en terme de sécurité, et peu de documentation publique.
- Les smartphones comportent plusieurs couches logicielles, chacune ayant des problématiques de sécurité différentes :

1. **Les pilotes des différents composants du téléphone :**

   Fournis par les différents constructeurs des composants, non-documentés publiquement

2. **Le système d'exploitation installé sur le smartphone :**

   Le système d'exploitation c'est l'ensemble des logiciels qui fait marcher le téléphone (ou l'ordi). On voit cela par la suite.

3. **Les applications installées par défaut**

   Souvent compliqué voir impossible à désinstaller / désactiver sans casser le smartphone.

4. **Les applications qu'on installe :**

Elles fonctionnent avec des permissions d'accès au téléphone. Que ce soit dans Android ou iOS, chaque application se donne des droits d'accès à ton téléphone. En tout il y a jusqu'à 150 permissions possibles, des applications telles que facebook en demande 58. Comme on regarde pas les permissions demandés, elles peuvent tout demander et y avoir accès comme bon leur semble au reste du téléphone.

4) Avoir un téléphone dont la carte SIM est « anonyme » [📞]

Il est possible d'avoir un téléphone « anonyme » en utilisant les cartes prépayés. On peut retrouver plusieurs marques : Lycamobile, Lebara, Syma (d'autres opérateurs en proposent, à tester).

Tu récupères une nouvelle carte SIM, et tu payes en liquide dans un bureau de tabac ton crédit qui permet de remplir le téléphone.

La première fois tu dois enregistrer ton téléphone : soit par téléphone, soit par internet. A chaque fois des données personnelles te seront demandées mais tu peux donner des informations imaginaires voir fantaisiste, il n'y a pas de vérifications. Si on te demande une photocopie de carte d'identité, tu peux mettre un faux ou une photo de montagne ça marche (à vérifier par opérateur), et si on te demande le numéro de ta carte d'identité tu dis le bon nombre de numéro mais tu les changes.

Parfois il faut un peu de temps (quelques heures) avant que ça soit effectif, c'est bien de préparer le téléphone à l'avance. Tu mets ensuite un code pour avoir un forfait. Par exemple tu peux très bien entrer 40 euros de crédit acheter dans un bureau de tabac, et avec le code il va te débiter chaque mois une partie du crédit jusqu'à ce qu'il n'y a plus assez (dans ce cas il faudra rentrer à nouveau du crédit).

Des fois faut chercher les meilleurs offres. Pour lycamobile par exemple, il faut taper *139*3004# pour avoir un forfait 5 euros par mois, téléphone et sms illimité mais pas d'internet, et *139*4099# pour avoir 10 euros d'illimité et un peu de forfait internet.

Petits typs à faire attention :

- Ne pas utiliser une carte SIM qui a été utilisée auparavant sous une identité qui t'es liée, ne pas mettre ta nouvelle carte SIM dans un téléphone que t'as déjà utilisé dans le passé.
- En cas de recherche la police peut savoir dans quel bureau de tabac a été acheté le forfait.
- Réfléchir au niveau d'anonymat que l'on veut. C'est déjà important et pas inutile d'avoir un téléphone qui n'est pas relié à ton identité car les recherches premières des flics se limiteront à faire une requête aux opérateurs pour connaître l'identité des personnes derrière un numéro IMSI ou IMEI. Ils peuvent mettre en place d'autres méthodes pour savoir qui est derrière un téléphone (mise sous écoute, étude des numéros contactés avec le téléphone, etc), ou peuvent mettre sous écoute tes proches pour trouver ton nouveau numéro lorsque tu les appelleras. Mais ça demande plus de moyens, donc ça dépend du modèle de menace.

Le problème c’est que le code de chiffrement est le même que le code de déverrouillage de l’écran, ce qui souvent force à faire des codes plus courts, car il faut le taper souvent. **Penser à éteindre un téléphone chiffré avant saisi pour activer le chiffrement**.

Si tu veux sauvegarder ton code quelque part, le mieux est d’utiliser un coffre fort à mot de passe comme keepassxc.

Réseau et chiffrement des communications

Au niveau du réseau il vaut mieux chiffrer ses communications en bout à bout (voir conseils d’applis) pour que le contenu ne soit pas divulgué, et pour cacher les sites internets fréquentés faire passer les applications par un vpn ou par le réseau Tor.

Activer la fonctionnalité « killswitch VPN ». Cette fonctionnalité permet d'éviter les fuites si le VPN est déconnecté. Elle se trouve dans ⚙ Paramètres → Réseau et internet → VPN → ⚙ → Bloquer les connexions sans VPN.

Désactiver les fonctionnalités non-utilisés

Quand c’est possible, désactiver les services Bluetooth et de localisation. Il y a parfois des interrupteurs à bascule pour l'appareil photo et le microphone. Lorsque vous ne les utilisez pas, il est mieux de désactiver ces fonctionnalités. Les applications ne peuvent pas utiliser les fonctions désactivées (même si elles ont reçu une autorisation individuelle) tant qu'elles ne sont pas réactivées.

Android

* Mode USB par défaut : charge uniquement
* Débogage USB désactivé
* Mettre un verrouillage d'écran rapide + un bon code de déverrouillage
* Désactiver l'identifiant de publicité ciblée qui récolte des données personnelles soit dans ⚙ Paramètres → Google → Annonces soit dans ⚙ Paramètres → Confidentialité → Publicités
* Chiffrement du téléphone (il est activé par défaut depuis android 10)
* Notifications discrètes
* Utiliser les Comptes d'Utilisateurs pour séparer certains usages, ou une application d'isolement d'applis telle que Insular ou Shelter

iOS

* Bon code de déverrouillage
* Désactiver les sauvegardes sur iCloud
* Désactiver l'identifiant de publicité
* Attention aux notifications

⇒ Le téléphone est chiffré* par défaut, mais parfois ce chiffrement est contournable.

Tableau de permissions possibles sur android :

- **Capteurs corporels** : obtenir des informations sur vos signes vitaux.
- **Agenda** : Lire / modifier / créer des évènements dans l’agenda.
- **Journaux d'appels** : consulter et modifier l'historique de vos appels.
- **Appareil photo** : utiliser votre caméra pour prendre des photos ou enregistrer des vidéos.
- **Contacts** : accéder à votre liste de contacts / la modifier.
- **Position** : obtenir la position (approximative par GSM ou wifi, ou exact par gps) de votre appareil.
- **Micro** : procéder à des enregistrements audio.
- **Appareils Bluetooth à proximité** : les applications peuvent détecter les appareils à proximité et s'y connecter.
- **Téléphone** : passer et gérer des appels téléphoniques, lire le statut du téléphone, la liste des appels, voir qui appelle, modifier la liste des appels, ajouter des messageries vocales, utiliser la VoIP (voix par internet), rediriger / suspendre des appels,....
- **Activité physique** : obtenir des informations sur votre activité physique (marche, vélo, nombre de pas, etc.).
- **SMS** : accéder aux SMS entrants et envoyer des SMS.
- **Stockage** : télécharger / modifier des photos et d'autres fichiers sur votre téléphone.

Dans le play store il y a beaucoup d’applications malveillantes (aussi appelées malwares). Par exemple si on prend une appli avec un compte craqué de spotify, on peut l’avoir gratuitement, mais c’est possible qu’en parallèle de spotify on ait installé un logiciel malveillant (ce qui veut pas dire que ça va donner des infos aux keufs, plutôt à des groupes qui vont revendre les infos pour faire de la maille).

Le système d’exploitation du smartphone 📱

Il en existe un certain nombre : Android, iOS, Windows, GrapheneOS, Blackberry, Ubuntu Touch, /e/, LineageOS, DivestOS, … En terme de sécurité, le mieux est **GrapheneOS** mais ne s’installe que sur des Pixel (voir chapitre changer de système d’exploitation). On va s’attarder ici sur les 2 principaux utilisés.

Problématiques spécifiques des 2 systèmes d’exploitation principaux sur smartphone

Apple

Ecosystème où la marque contrôle tout. C’est les ingénieurs apple qui font iOS (le système d’exploitation) et qui conçoivent les téléphones, les commerciaux apple qui

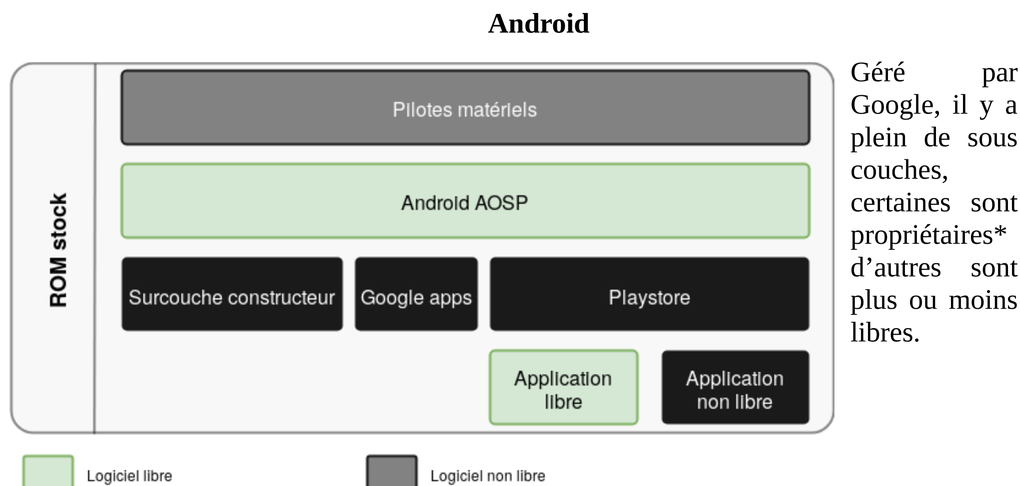
les diffusent, et les magasins apple qui les vendent et les réparent. Apple contrôle tout de la conception à la commercialisation, aux mise à jour, à l'après vente…

Problématique : Ce système d'exploitation ainsi que ses applications sont propriétaires*. Apple rechigne a sérieusement protéger les données des usagers lorsque les keufs états-uniens demandent.

Avantages : les mises à jour du système sont suivies plus longtemps, le matériel est de bonne qualité, le système est cohérent et fonctionne bien.

Apple travaille régulièrement avec le FBI, même s'ils disent qu'ils sont sécurisés. Pour un hacker c'est compliqué de rentrer dans un iOS, mais pour les flics américains il y a des possibilités.

Android



Géré par Google, il y a plein de sous couches, certaines sont propriétaires* d'autres sont plus ou moins libres.

- Google a programmé Android une base libre* (AOSP, après l'avoir rachetée), mais pour rendre fonctionnel son système, il faut rajouter des bases google non-libres* (GCM/FCM, play store, service de géolocalisation, youtube, etc.).
- Par dessus ça les fabricants de téléphones (Samsung) prennent android + logiciels google et ajoutent leurs merdes (samsung quies, MiUI, …)
- Il y a des morceaux de logiciels des fabricants de composants (souvent propriétaires*), comme les pilotes wifi ou d'autres trucs.
- Les opérateurs téléphoniques rajoutent aussi parfois des trucs, comme Orange Music ou autres

Cela pause le problème que si un des acteurs ne fournit pas les mises à jour, c'est pas possible de faire la mise à jour sur le smartphone. Beaucoup de téléphones sous Android n'ont plus de mises à jour rapidement après leur lancement. Cela signifie que les failles de sécurité découvertes dans le temps ne sont pas corrigées.

de Signal utilisent des morceaux de code de Google qui sont propriétaires (l'inverse de libre).

Il existe des applications qui reprennent le code-source de Signal pour en modifier les parties libres. Le protocole d'échange étant le même, il est possible d'échanger un message Signal depuis une de ces applications alternatives.

Molly et Molly-FOSS

Comme Signal, Molly utilise les parties de code propriétaires issues de Google. Cependant, Molly propose quelques options que Signal n'a pas : - avoir un code de de déverrouillage de l'application différent du code utilisé pour verrouiller le téléphone - programmer des sauvegardes

Molly- est une tentative de la communauté autour de Molly de rendre l'application 100% libre, donc proposer une application qui soit libérée des morceaux de code appartenant à Google.

Plus d'informations sur le site de l'application[22].

Session

Session est un fork* de Signal qui a créé son propre protocole de communication, pour le rendre non-centralisé. Ça veut dire que tous les messages ne doivent pas nécessairement passer par les serveurs de l'application mais l'ensemble des serveurs qui hébergent les utilisateur·rices. Cependant, Session base son réseau sur Lokinet, qui dépend de la blockchain, et beaucoup préféreront rester éloigné·es de ça, parce que cette technologie trouve ses bases dans l'idéologie libertarienne (un capitalisme certain opposé à toute forme de régulation).

3) Paramètres du smartphone 📱

Un bon code de chiffrement du téléphone

On va éviter la reconnaissance faciale (problématique en tant que technologie et y a des failles) et emprunte digitale (c'est possible de forcer la personne à mettre son doigt). Les schémas, souvent il reste des traces sur l'écran qui permet de les refaire.

Phrase de passe: le mieux en terme de sécurité mais ça peut devenir pénible à taper (adapter le temps de verrouillage de l'écran).

Digicode: bien à condition d'en avoir un assez long. C'est encore mieux si on active l'option "disposition aléatoire" disponible sur certains systèmes. La longueur du mot de passe dépend du type de téléphone. Recommandation minimale sur un modèle tel que graphen os : 8 chiffres sur un clavier disposé aléatoirement.

22 https://molly.im/

- Vérifier les appareils associés régulièrement (si Signal a été installé sur un ordinateur ou un autre téléphone, il s'affiche dans la liste des appareils reliés)

AUTRES

- Numéro de sécurité à vérifier avec ses correspondant·es (flasher un QR code sur le téléphone de son contact quand on le croise en vrai)

PARAMÈTRES/STORIES

- Désactiver les confirmations de vues sur les stories
- Désactiver les stories si on ne s'en sert pas et qu'on ne consulte pas les stories des gens

En cas de réquisition judiciaire faite à Signal, Signal promet ne posséder que la date de création du compte ainsi que la date de la dernière connexion au compte : sur leur site on peut retrouver ce que Signal dit fournir aux institutions judiciaires : https://signal.org/bigbrother/.

=> Tutoriel - Quelques configurations de signal avec des impressions d'écran sur ce site: https://ssd.eff.org/fr/module/guide-pratique-utiliser-signal

Avoir signal sur ordinateur

Il est possible d'installer signal-desktop sur ordinateur quelque soit le système d'exploitation. Il faut scanner le QR à partir d'un smartphone et activer de temps en temps le téléphone, mais ça peut permettre de consulter ses signal dans certains lieux sans avoir à borner avec le téléphone. On peut aussi utiliser un smartphone en mode avion connecté par wifi, mais il est plus compliqué techniquement de ne pas relier le téléphone à la boxe ou au partage de connexion.

Il est aussi possible d'utiliser signal sur ordi sans smartphone avec un téléphone à touche grace à signal-cli. Il faut l'installer avec une personne qui a des compétences informatiques, et s'il faut le maintenir dans les années avoir le contact d'une telle personne pour certaines mises à jour[21]. Une fois le compte ouvert, s'il est connecté au moins une fois par mois, il n'y a plus de lien entre le téléphone et l'ordinateur.

Il peut y avoir 2 comptes signal sur un ordi, soit en installant la version signal-desktop beta en parallèle de la version classique, attention la version beta peut être soumis à des instabilités de fonctionnement car elle n'est pas complètement vérifiée. Soit avec des compétences techniques en fouillant sur internet.

Utiliser Signal sans Signal

Signal est une application qui n'est que partiellement libre (open-source et dont la reproduction, la modification et la diffusion sont libres). Certaines parties du code

21 Tutoriel : https://kemenaran.winosx.com/posts/signal-sans-smartphone

II) Les problèmes inévitables de sécurité dans les téléphones [📞]

Ce qu'on ne peut pas actuellement résoudre avec les téléphones :

Géolocalisation du téléphone [📞]

Un téléphone allumé (même sans carte SIM) est géolocalisation très simplement par les entreprises qui contrôlent les antennes (et donc les keufs peuvent leur demander certaines infos).

En théorie, dans un environnement plat, la géolocalisation est précise à 50 cm en 4G, quelques m à quelques 10aines de m en 2G et 3G (mais on a pas tout le temps ces conditions théoriques), et la 5G est sensée permettre une localisation infiniment plus précise. Cette géolocalisation est indépendante du GPS. Le mode avion coupe toute connexion aux antennes, donc la localisation par l'opérateur devient impossible.

Différents types de localisation par smartphone

Le fonctionnement du GPS : Les satellites émettent leur positionnement. Activer la localisation c'est demander au téléphone de capter ces signaux et ainsi savoir avec précision où il se situe (être sous terre ou dans un bâtiment peut fausser ou rendre impossible la localisation). Les applications peuvent récupérer cette localisation qui a une précision de quelques mètres, mais les satellites n'ont pas connaissance de la localisation des appareils.

Antennes Téléphoniques (2G, 3G, 4G, 5G) : le téléphone et les antennes sont continuellement en communication, dès lors que ce premier est allumé (et pas en mode avion, carte SIM ou pas). Les antennes ont connaissance de la distance à laquelle se trouve un téléphone, donc un rayon autour de l'antenne. Une triangulation avec 3 antennes permet une localisation. Sans cette triangulation la précision est faible (plusieurs 100 aines de m)

Localisation par wifi : le téléphone est localisé par la position connue des réseaux wifi

Appels et SMS en clair [📞]

Les appels et SMS qu'on envoie passent en clair* dans le réseau. C'est à dire que leur contenu ainsi que les métadonnées* les concernant sont interceptables. Dans la réalité, c'est un peu plus compliqué car les communications ont un chiffrement, mais ce chiffrement est fait pour être désactivable par des acteur.ices étatiques. Que ce soit en 2G, 3G, 4G, ou 5G.

Ce qui intéresse principalement les flics c'est les métadonnées, car ça leur permet de faire des graphes relationnels, de savoir qui est « au centre » d'un groupe, etc.

Conditions pour que le téléphone ne communique plus avec les antennes

En mode avion, les téléphones ne communiquent plus avec les antennes et donc il n’y a pas de géolocalisation possible de la part des antennes. Cependant on peut imaginer des logiciels malveillants qui récolteraient la géolocalisation via le GPS et la transmettraient lorsque le tel se reconnecte au réseau.

Éteint, le téléphone ne communique pas avec les antennes. Cependant il peut parfois se rallumer, par exemple certains téléphones s’allume quand un réveil se déclenche. Ou notre poche peut appuyer sur le bouton d’alimentation du tél… On peut aussi imaginer un logiciel malveillant installé dans le téléphone qui le rallume ou fait croire qu’il est éteint. Même si ça ne semble pas être fréquent, pour se protéger de cela, le top est d’enlever la batterie. Certains modèles de téléphone ne permettent pas d’enlever la batterie. On peut aussi enrouler le tel dans une quinzaine de couches d’alu alimentaire, histoire de bien l’isoler des ondes.

Attention, un téléphone allumé sans carte sim se connecte quand même au réseau téléphonique, afin de pouvoir appeler les secours. En france cette fonction a été désactivée par la plupart des opérateurs il y a de nombreuses années, mais le téléphone peut se connecter tout de même au réseau.

Identification des téléphones [📞]

IMEI / IMSI

Lorsque le tel se connecte à une antenne, il transmet les identifiants IMSI des cartes SIM actives, les identifiants IMEI du téléphone, le modèle du téléphone et l’opérateur téléphonique utilisé. L’IMSI (pour « Identifiant d’abonné·e mobile international ») est l’un des identifiants permettant à l’opérateur de vérifier que la carte SIM a le droit de communiquer sur son réseau.

Le numéro IMEI (pour « identifiant d’équipement mobile international ») est un identifiant unique par emplacement de carte SIM de chaque téléphone. Il est lié à la marque du tel ainsi qu’au modèle précis, parfois même à la couleur de la coque. C’est lui qui sert à bloquer un tel quand il est déclaré volé (même si c’est rarement mis en place).

Cet identifiant est stocké de manière définitive dans le téléphone. Contrairement aux adresses MAC des cartes WiFi ou ethernet des ordis, on ne peux pas usurper l'identifiant IMEI d'un téléphone (enfin c’est *presque* impossible, bien que des possibilités commencent à voir le jour). On peut connaître les numéros IMEI d’un tel en composant le *#06#. L’IMEI est une suite de 15 à 17 chiffres qui comprend :

- Les deux premiers chiffres indiquent le pays de fabrication
- Les six chiffres suivants représentent le numéro de série
- Le dernier chiffre est un chiffre d’authentification et sert donc de clé de sécurité.

personnes par Signal. On peut aussi le mettre en description (“À propos”) pour que nos contacts l'aient rapidement.

PARAMÈTRES/COMPTE (important)

- Mettre un NIP (⚠ lire la notice) et activer blocage d’inscription.

PARAMÈTRES/CONVERSATIONS

- Désactiver l'option « Aperçus de liens ».
- Créer des dossiers de conversation, si on utilisez beaucoup Signal, ça permet de séparer des « types » de conversations ou de contacts (pratique pour l’organisation mentale).

PARAMÈTRES/CONFIDENTIALITÉ

- Numéro de téléphone : « Qui peut voir mon numéro » : personne (par défaut).
- « Qui peut me trouver grâce à mon numéro » : possible de mettre personne (⚠ plus personne ne pourra nous trouver sur Signal via notre numéro, et des gens pourraient nous contacter en clair pensant que nous n’avons pas l’application).
- Désactiver les confirmations de lecture (le double-coche qui devient blanc en bas à droite d’un message envoyé – les destinataires ne recevront plus cet accusé de lecture, et ceux des autres ne s'afficheront plus).
- Désactiver les indicateurs de saisie (les 3 points qui montrent que quelqu’un est en train d’écrire).
- (**Important**) Activer les messages éphémères et mettre une valeur par défaut (ex : 1 semaine).
- Activer la sécurité d’écran (verrou d’écran) : pour ouvrir l’application il faut remettre son code de déverrouillage de téléphone.
- (**Important**) Activer un verrouillage automatique de l’écran avec un temps qui correspond à son modèle de menace (et prendre l’habitude de le modifier selon les contextes) : c’est le temps que met le téléphone à reverrouiller l’application.
- (**Important**) Activer l’option « Clavier incognito »
- (**Important**) Activer la sécurité de l’écran (empêche les captures d’écran pour soi-même = si quelqu’un prend le téléphone, il ne peut pas rapidement faire une capture et se l’envoyer + ça permet d’éviter que le contenu de Signal n’en sorte et se balade dans les dossiers d'images de son téléphone)
- S’assurer que les notifications n’affichent rien si le téléphone est verrouillé

PARAMÈTRES/CONFIDENTIALITÉ/PARAMÈTRES AVANCÉS (important)

- Activer l’option « Toujours relayer les appels » (important de comprendre les implications : ça permet de ne pas divulguer l’adresse IP de notre connexion aux destinataires de nos appels)

PARAMÈTRES/APPAREILS ASSOCIÉS

Autres

Une série d'applis biens et dispo dans F-Droid: Fossify (https://www.fossify.org/). Avant ça s'appelait Simple Mobile Tools mais le créateur a vendu à une boîte de merde, donc des gens on repris le projet l'ont renommé pour lui donner une seconde vie! (c'est la force du logiciel libre). Il y a un calendrier, un gestionnaire de contacts, une appli SMS, une appli de notes, une galerie, etc.

Un certain nombre d'applis ont des versions ordinateurs – à prendre en considération pour avoir des communications ordi-téléphones :

- Signal (Signal-desktop, axolotl.chat)
- Conversations, compatible avec Dino, Pidgin, Gajim, etc
- Element (https://element.io/get-started)
- etc etc

Revenons sur Signal

Défauts

- Possible sensation de sécurité parfaite (illusoire)
- Centralisé (protocole utilisable uniquement sur cette application ou ses forks* et sur leur serveur)
- Pour s'inscrire, il faut le lier à un numéro de téléphone souvent relié à une identité réelle (même si plus visible pour les utilisateur.ices)
- Idéologies cheloues (intégration de cryptomonnaie, refus de décentraliser…)
- Modèle économique douteux : certain.es développeur·euses sont payé·es 600 000 dollars par an ; l'application n'est pas rentable, est en déficit et reçoit des apports d'argent douteux ; double discours en fonction de si Signal s'adresse à ses investisseurs ou à son public.
- Il est fort possible que leur modèle économique soit basé sur un potentiel : l'idée est d'avoir une masse critique d'usagèr·es pour changer radicalement de politique interne (rajout de pubs ? changement de niveau de sécurité ? revente ?). Comme X, Whatsapp, ou équivalents, le jour où il y aura plus de 100 millions d'utilisateur·ices, si le changement de politique en fait partir plusieurs millions, Signal pourra continuer.

Options à configurer

PARAMÈTRES/PROFIL (important) :

- Nom ; À propos ; Photo de profil → rester anonyme le plus possible.
- Ajouter un nom d'utilisateur.ice (@XXXXX.NN), se terminant nécessairement par un point et 2 chiffres. Cet identifiant permettra d'être retrouvé·e sur Signal par les autres utilisateur·rices. Il n'est pas visible par défaut, il faut penser à le demander ou l'envoyer pour mettre en lien des

En france, les opérateurs gardent les infos de connexion pendant 1 an. Ça veut dire que l'information que quel IMSI était dans quel IMEI est gardée tout ce temps. Avec ça est aussi gardée la liste des antennes auxquelles s'est connecté un tel ainsi que les dates et heures correspondantes. D'autres infos sont gardées mais on en parlera plus tard.

Il est donc facile pour les opérateurs (donc les keufs) d'avoir la liste des téléphones ayant servis pour telle carte sim ou tel numéro de tel, ainsi que la liste des cartes SIM ayant été branchées dans tel téléphone.

S'il y a plusieurs emplacements SIM dans un même téléphone, il faut considérer qu'ils sont liés entre eux. Sur internet[4] on peut trouver les différents IMEI d'un même téléphone et parfois aussi la couleur de la coque, la marque, les dimensions, les informations basiques du téléphone, etc… Donc s'il y a 2 cartes SIM dans un même téléphone, les opérateurs peuvent facilement savoir que c'est le même téléphone qui utilise les 2 cartes SIM.

Les opérateurs téléphoniques ont légalement une obligation de supprimer ces informations d'identification au bout d'un an. On n'a pas d'assurance à 100% que cela soit fait, de plus si les infos des opérateurs ont été donné à des services de renseignement tels que la DGSI (Direction Générale de la Sécurité Intérieur), c'est probable que cette dernière instance va garder les données plus longtemps.

A partir du numéro de téléphone il peut être possible d'estimé l'opérateur chez qui t'es, les 4 chiffres après le 06 / 07 sont attribués à ceux-ci[5]. Cependant avec la « portabilité » des numéros ça peut être plus compliqué que cela, car il est possible de changer d'opérateurs en gardant le même numéro.

3179 où comment se faire identifier rapidement à partir de son tel

Si un téléphone appel le 3179, il reçoit par vocal puis par sms à minima son RIO (Relevé d'Identité d'Opérateur). Il est composé d'une suite de chiffres et lettres donnant ces infos:

1. Les deux premiers chiffres indiquent l'**opérateur concerné** (01 pour Orange et Sosh, 02 pour SFR, 03 pour Bouygues et B&You...)
2. La lettre suivante indique le **type de client** (E pour Entreprise et P pour Particulier)
3. Les 5 caractères suivants indiquent le **numéro de contrat** auprès de l'opérateur
4. Les 3 derniers caractères constituent le **code de contrôle** pour vérifier la correspondance entre le RIO et le numéro de la ligne mobile.

4 Pour voir ces infos, rendez vous sur ce site : https://www.imei.info/

5 Vois la liste des préfixes des opérateurs téléphoniques : https://fr.wikipedia.org/wiki/Liste_des_pr%C3%A9fixes_des_op%C3%A9rateurs_de_t%C3%A9l%C3%A9phonie_mobile_en_France

Qui plus est, chez certains opérateurs il est envoyé aussi le nom et prénom de la personne indiqué à l'opérateur. Dans certains coin c'est utilisé par des contrôleurs pour vérifier l'identité donnée. Information à avoir en tête lorsque tu dis que tu as ton téléphone. Tu peux vérifier en amont sur ton téléphone quelles informations arrivent sur ton téléphone via cette opération. Les opérateurs prépayés type lyca ne renvoient que le RIO.

Factures détaillées ou fadettes

Il s'agit de toutes les informations autres que le contenu même de la conversation : les fadettes mentionnent les numéros, dates, heures et durées de communication. Les opérateurs gardent les « factures détaillées » (ou FADET / fadettes) pendant 5 ans car c'est une autre législation : c'est de la législation fiscale. Ce temps correspond au délai de contestation possible des factures. Mais le cadre légal ne permet en théorie pas aux flics d'en demander l'accès au-delà **d'un an**. Cependant dans le cadre d'une enquête passée certaines données peuvent être mises dans un dossier et dans ce cas être utilisées plus tard.

30 000 flics ont accès depuis juin 2022 au logiciel *DeveryAnalytics Telephony Data* qui permet d'aider à l'analyse de fadettes et autres données de masse[6].

Des nouvelles jurisprudences de la cour de cassation du 12 juillet 2022 peuvent permettre de contester dans certains cadres l'utilisation dans les procès de preuves obtenues à partir de fadettes.[7]

Failles de sécurité et mises à jour 📱

Aucun logiciel n'est parfait, tant qu'il y aura des logiciels, il y aura des failles de sécurité. L'existence de failles ne veut pas dire que des personnes les exploitent, mais il faut garder à l'esprit que de tout temps les logiciels ont été attaqués, et le seront encore. Même les meilleurs logiciels de sécurité, même quand c'est les meilleurs ingénieur·e·s du monde qui ont bossé dessus.

Quelques exemples de failles de sécurités découvertes ces dernières années :

En 2015 : sur Android, on pouvait recevoir un MMS trafiqué qui donnait accès aux audios et vidéos et la carte SD du téléphone.

En 2019 : sur iOS, 4 failles de sécurité permettaient de prendre le contrôle d'un téléphone en amenant l'usager·e à se connecter à un site internet malveillant ; sur Android, il était possible de déclencher une réponse à un appel Signal [8]

6 Le site internet du producteur de logiciel: https://deveryware.com/marches/securite-interieure/data-analytics/

7 https://www.courdecassation.fr/toutes-les-actualites/2022/07/12/enquetes-penales-conservation-et-acces-aux-donnees-de-connexion

8 Source: https://www.cvedetails.com/cve/CVE-2019-17191/

- TowerJump
- Puzzles (plein de casse-têtes trop stylés)
- Rabbit Escape
- Sokoban
- Shattered Pixel Dungeon (exploration)

Podcasts

- AntennaPod

Horloge

- Horloge fossify

Sécurité

- **Hypatia Antivirus** pour Android, vous permet de scanner vos documents et votre système afin de détecter la présence de virus connus
- Extirpater (effacer l'espace disque disponible) - Écrase la mémoire libre du téléphone (shred) permet de s'assurer que même lorsqu'on supprime des documents sur le tel, il sera difficile pour quelqu'un de les récupérer. Attention pour des documents vraiment sensible, à cause du fonctionnement de la mémoire du téléphone, des données peuvent subsister dans d'autres partis du téléphones.
- Duress (réinitialisation du téléphone sur code de déverrouillage spécial)
  - **ATTENTION**: Duress utilise les services d'accessibilité, donc pour les versions antérieures à Android 10, il désactive le chiffrement du téléphone pour marcher !
- Wasted (Permet d'autodétruire votre téléphone en cas de panique. L'appli va formater et réinitialiser l'OS et, une fois l'opération finie, on aura un téléphone tout propre :) /!\ Pour garantir la sécurité de vos données effacées il faut impérativement que votre téléphone soit chiffré avant de l'autodétruire.) Pensez à gérer vos sauvegardes !
- AirGuard, application pour détecter les Airtag, qui sont des petits traqueurs matériels faciles à trouver dans le commerce [défense spécifique].

Séparations des comptes sur smartphone

- Sur beaucoup d'Android et notamment les versions 10 et plus, il est possible d'activer les “Comptes d'utilisateur”, qui permettent d'avoir une séparation plus rigide des applis. Ainsi ça rend compliqué pour une appli de chopper les infos d'une autre appli sur un 2nd compte. Quand on utilise un système d'exploitation tel que GrapheneOS ou LineageOS, on peut activer cette fonctionnalité, installer F-Droid dans tous les profils et n'utiliser Aurora Store (et des outils google) que dans un profil dédié.

- Etar – OpenSource Calendar
- DAVx^5 (synchronisation de calendrier distant, avec Nextcloud par exemple. Compatible avec fossify Calendar, simple calendar ou Etar)

Notes

- Fossify Notes (hors-ligne, avec un super widget)
- Nextcloud Notes (pour synchroniser avec un nextcloud)
- Standard Notes : notes chiffrées de bout en bout en local et sur le cloud (dispo en version ordi aussi)

Pare-feu

- Netguard (impossible de l'utiliser en même temps qu'un VPN)

Isolation d'applis

- Insular
- Shelter

Navigation web

- Mull (via FFUpdater (dans F-Droid), ou dans F-Droid via les dépôts de DivestOS. Installer le plugin Ublock Origin pour bloquer les pubs)
- Firefox Focus (via l'appli FFUpdater ; inclus un bloqueur de pubs et de pisteurs)
- Tor Browser
- DuckDuckGo Privacy Browser

Alternatives à Youtube/Bandcamp/Soundcloud/Framatube

- NewPipe (à installer depuis les dépôts de Newpipe en scannant le QR-code dans les paramètres de F-Droid) ou PipePipe (Très léger mais expose votre adresse IP aux serveurs de google)
- LibreTube (similaire à Newpipe mais se connecte à https://piped.kavin.rocks et donc ne contacte jamais directement Google)

Cartes

- Organic Maps (basé sur Openstreepmap)
- OsmAnd (idem)
- GMaps WV (pas le top, mais isole une page web pour accéder à GoogleMaps)

Sauvegarde

- Seedvault (pas hyper simple à utiliser)
- Faire des sauvegardes manuelles…

Jeux

- Lona (sorte de snake arondi)

En 2020 : sur Android 8 et 9 et la plupart des Linux, avec le bluetooth allumé mais non connecté, un.e attaquant.e pouvait prendre le contrôle et aspirer toutes les données. Cette faille a été corrigée, mais bon nombre de téléphones n'ont juste jamais de mises à jour et sont donc toujours vulnérables… Pour s'en protéger il faut couper le bluetooth.

Comme déjà dit, des failles de sécurité seront toujours découvertes. Parfois corrigées avant d'être rendues publiques, parfois utilisées par des adversaires pendant plusieurs années avant d'être corrigées. C'est pourquoi il est extrêmement important d'appliquer les mises-à-jour au maximum, que ce soit sur nos ordis ou nos téléphones. Il est important que les applications et le système d'exploitation qu'on utilise soient suivies dans le temps, que l'équipe de développement corrige les failles de sécurité découvertes. En terme de confiance, on peut se renseigner sur la réactivité et les développeur.euses lorsqu'une faille est connue et la communication qu'iels en font. Ça peut être déterminant sur le choix du système d'exploitation ou des applis.

On peut savoir combien de temps sont suivis pas mal de modèles de téléphones sur ce site : https://endoflife.date

Données de la carte sim et du téléphone [📞]

En cas d'accès physique à la carte SIM et au téléphone :

- Activer le code PIN de la carte SIM peut rendre plus compliqué à des flics de base l'accès à certaines informations. Cependant, ce code PIN est aisément contournable grâce au code PUK que les flics peuvent demander aux opérateurs. Il n'est pas possible de protéger de manière sûre les données stockées dans une carte SIM (IMSI, contacts, …).

- Les données d'un téléphone non-chiffré* sont accessibles par des outils que nous verrons dans le chapitre suivant.

Communiquer c'est à plusieurs [📞]

La communication c'est généralement un truc qui se fait à plusieurs. Les outils et pratiques qu'on choisit d'utiliser de son côté ne sont pas forcément les mêmes chez les autres. Si j'ai le téléphone le plus sécurisé du monde, mais que des potes m'appellent pour me demander si je vais à telle réunion ce soir, leurs pratiques peuvent rendre les miennes caduques.

- Ne pas se sentir infaillible parce qu'on chiffre son tél ou qu'on a des bonnes pratiques de son côté.
- Les pratiques collectives sont à discuter ensemble et il est important de se soutenir dans la mise en place d'outils.
- Dans la suite il y a un certain nombre de conseils d'autodéfense numérique, ça peut être plus confort d'y aller par pallier pour que ça soit abordable petit à petit.

III) Outils des keufs

On a des éléments de pratiques utilisées dans des dossiers judiciaires pour tout ce qui touche au domaine policier, mais il est compliqué de connaître les pratiques réelles des services de renseignement[9].

Interceptions administratives et judiciaires [📞]

La police peut faire des réquisitions auprès des opérateurs, soit pendant un évènement, soit après coup. Une panoplie de choix est à leur disposition[10], ça peut s'appliquer :

- sur une antenne en particulier : identifiants IMEI et/ou IMSI, modèle du téléphone, opérateur téléphonique ayant borné à telle antenne à tel moment.
- sur un téléphone ou un carte SIM spécifique : données fournies à l'opérateur – comme l'adresse mail, les coordonnées bancaires ou l'identit, historique des cartes SIM mises dans tel téléphone, liste des téléphones ayant servis à telle carte SIM, le modèle du téléphone utilisé, les factures détaillées (voir partie associée), le code PUK (permet de déverrouiller le code PIN de la carte SIM), mise sous écoute en temps réel (cela renvoie en parallèle l'appel sur le téléphone d'un flic), la géolocalisation en temps réel, les sites consultés (pas toujours possible, et dans beaucoup de cas ça ne concerne que les noms de domaines visités, pas les pages exactes), etc.
- pour faire de l'identification en masse : les keufs demandent l'identité associée à plusieurs centaines de numéros de téléphones d'un coup. Les délais de réponse sont de l'ordre de l'heure.
- faire une recherche auprès de chacun des opérateurs pour obtenir le numéro de téléphone à partir de l'identité d'une personne. Ça nécessite pour les flics de vérifier les numéros récupérés par cette méthode (homonymes, faux noms…) ça n'est pas pratique d'usage pour eux.

Une plateforme a été créé pour automatiser, conventionner les tarfis et fluidifier le travail avec les opérateurs : la PNIJ, pour plateforme nationale des interceptions judiciaires (résultat d'un partenariat public-privé avec Thales)[11]. Légalement la

9 Il est possible de fouiller dans les rapports de a CNTCR - Commission nationale de contrôle des techniques de renseignement pour avoir les infos qu'ils veulent bien nous fournir : https://www.cnctr.fr/8_relations.html

10 On peut s'amuser à fouiller parmi les différentes possibilités offertes aux flics, avec les prix de chaque opération ici par exemple pour la date de 2016 : https://docplayer.fr/72431284-Memoire-recapitulatif-de-frais-de-justice.html

11 Dans un commentaire du ministre de la justice fin 2018 qui donne l'ampleur de la plateforme : « La PNIJ est ainsi aujourd'hui, pleinement opérationnelle et utilisée par plus de 60 000 magistrats, enquêteurs et greffiers. Elle traite plus de 11 000 interceptions simultanées et 6 000 demandes de prestations annexes par jour. Elle intercepte près de 800000 communications et 1,2 million de SMS par semaine. » https://questions.assemblee-nationale.fr/q15/15-13319QE.htm

Autres applis de sécurité

- exodus privacy : εxodus analyse les applications Android dans le but de lister les pisteurs embarqués. Un pisteur est un bout de logiciel dont le but est la collecte de données à propos de vous et de vos usages. Ainsi, les rapports d'εxodus vous révèlent les ingrédients du gâteau. Disponible aussi sur F-droid. Ne marche pas pour les applis payantes. Ne marche pas sur certains pisteurs qui sont limités à certaines zones géographiques ou qui se lancent longtemps après le démarrage de l'application. Un podcast ici explique comment fonctionne les traqueurs ainsi qu'exodus privacy.
- Hypatia : Scanner de malware, fonctionne hors internet : https://github.com/Divested-Mobile/Hypatia/blob/stable/README.fr.md
- Ente Auth : application pour avoir une double authentification

Photos

- Open Camera
- Obscuracam : qui peut être configuré pour flouter les visages automatiquement.
- Scrambled Exif
- Cryptocam + OpenKeyChain (chiffrement direct des photos et vidéos avec OpenPGP. Nécessite « Cryptocam Companion /CLI » pour ouvrir les vidéos dans l'ordi. Demande quelques connaissances et un peu de lecture de tutoriels en anglais, sur https://cryptocam.gitlab.io)

Vidéos / musique

- VLC
- Vanilla

Lecture de documents

- Secure PDF Viewer (Par défaut sur GrapheneOS), nécessite Android 12, vraiment sécurisé)
- Librera (pour lire des ebooks)
- MuPDF (pour afficher PDF et autres)

Bonus : pleins de ebooks à télécharger sur trantor.is, z-lib.org, libgen.rs ou fourtoutici.ac

Audio/visio-conférence

- Jitsi (audio/vidéo à plusieurs)
- Plumble (protocole Mumble, audio uniquement)
- Appels Signal
- Wire (à 2)

Calendrier/agenda

- Fossify Calendar (fonctionne hors-ligne)

- Cwtch (https://cwtch.im/)

Il existe aussi un comparateur d'applications fait par le site nothing2hide de communication sur plusieurs critères intéressants (attention il y a quelques erreurs dans le comparateur par exemple le code source du serveur de telegram n'est absolument pas libre ni opensource par exemple). Cette page compare les logiciels : briar, conversations, delta chat, Element, Imessage, Jami, Signal, Télégram, Threema, Whatsapp, Wire sur la sécurité et vie privée, la durabilité, les fonctions et les modes de stockages : https://wiki.nothing2hide.org/doku.php?id=formations:smartphones:app-communications-securisees

On trouve aussi des gens qui râlent (à raison) sur Signal et comparent d'autres applis: https://md.lqdn.fr/s/9tEgRhfkL#

Applis visant à protéger l'identité de leurs utilisateurices

- Tor Browser (pour naviguer sur le web)
- Briar (pour échanger des messages instantanés chiffré sans donner de numéro de tel ou d'e-mail)
- Conversations (pour échanger des messages instantanés chiffré)

Pour les SMS

- QUIK SMS (anciennement QKSMS)
- Fossify SMS Messenger
- l'appli de SMS de base d'Android Open-Source Project

Pour les e-mails

- K-9 Mail
- FairEmail

→ Ces deux clients permettent de chiffrer les e-mails avec PGP à l'aide de OpenKeyChain.

VPN

- Version gratuite : RiseupVPN (prix libre / gratuit), proton, neutrinet
- Mullvad VPN – bien en terme de confidentialité et rapidité (payant, 5 euros par mois pour 5 comptes, possibilité de payer en liquide)
- CalyxVPN
- Orbot : pour configurer d'autres applis pour les faire passer par tor (ne marche pas pour toutes les applis), ni avec l'utilisation en parallèle d'un pare-feu (firewall) tel que NetGuard

Coffre fort à mot de passe

- Keepassxd

demande des flics doit passer par cette plateforme, dans la pratique et aussi parce que la PNIJ n'a pas de contrat avec tous les opérateurs, 25 % des demandes ne passent pas par la PNIJ[12].

Données faciles à obtenir à distance par la police

- Données d'identification
- Identifiant carte SIM
- Factures détaillés
- Mise sous écoute (plus coûteuse en terme financier)

Bornage et géolocalisation

Si les opérateurs téléphoniques doivent conserver les antennes auxquelles se sont connectées un téléphone – et donc une géolocalisation approximative – ils ne sont pas tenus de garder automatiquement les localisations des simples émissions des téléphones pour le localiser. Pour l'opérateur, il y a une localisation associé à chaque sms, appel ou data-paquet (c'est à dire toutes connections téléphones à internet) envoyés ou reçus. Hors géolocalisation en temps réel et hors IMSI catcher, les localisations obtenus par réquisitions par la police sont liés à des communications (à d'autres téléphones ou à des serveurs).

En garde à vue / audience / instruction / enquête 📱

Lors d'une garde-à-vue, notre droit au silence est limité par l'« obligation de fournir la convention de chiffrement ». Cette obligation s'applique notamment aux téléphones, si la demande est faite dans son cadre. Dans ce cas, refuser de donner les mots de passe, peut amener en soi un risque de procès. Le cadre permettant qu'une telle demande nous soit faite est le suivant :

- la demande doit être fait par un opj (Officier de Police Judiciaire, pas un flic « de base ») supervisé d'un magistrat – procureur ou juge d'instruction.
- elle doit être justifiée, il doit être démontré que le téléphone utilise des méthodes de cryptologie, et que le déverrouillage pourrait permettre d'accéder à des éléments pertinents pour avancer dans l'enquête en cours (« l'enquête ou l'instruction doivent avoir permis d'identifier l'existence des données traitées par le moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit »). S'il ne semble pas y avoir d'enquête approfondi, il ne devrait pas être possible d'y avoir condamnation pour cela.
- il faut qu'il soit démontré que tu connaisses ce code de déverrouillage.

12 Rapport du sénat du 15 novembre 2023, « Surveiller pour punir ? Pour une réforme de l'accès aux données de connexion dans l'enquête pénale »

Tout cela doit être explicitement formulé pour que ça soit accepté dans un cadre légal. Si l'évolution judiciaire ne va pas dans le bon sens au court du temps, **il reste toujours conseillé d'appliquer les mêmes règles qu'habituellement en garde à vue « je n'ai rien à déclarer » en cas de demande de code de déverrouillage** (et pas « je sais pas » ou autre)[13]. Ces poursuites ne semblent pas fréquentes, et c'est souvent utilisé comme chef d'inculpation qui en complète d'autres. L'avantage d'exercer ton droit au silence c'est que tu pourras choisir ta défense en cas de poursuite, bien des possibilités peuvent exister.

Le Kiosk – extracteur de téléphone 📱

Fabriqué par l'entreprise israélienne « Cellebrite », le Kiosk est vendu à des acteurs étatiques. C'est une version tout- compris de leur outil « UFED ». 500 kiosk ont été achetés en France pour les flics, à 8000 euros l'unité, installés d'ici 2023 (d'après des sources de 2020). Du coup ça n'est pas utilisé tout le temps. C'est un ordi tactile, avec des gros boutons et plein de câbles : il va essayer d'aspirer le contenu du téléphone et de générer des rapports valables aux yeux des magistrats (analyse forensique). Sur leur site on peut trouver les « release notes »[14], contenant des listes de téléphones qu'ils arrivent à craquer, des listes d'applis prisent en charge par l'extraction de données, et d'autres infos inquiétantes.

Pour fonctionner, l'UFED exploite des failles de sécurité présentes dans la partie du système d'exploitation qui gère le port USB. Ces failles de sécurité peuvent être déjà publiques ou découvertes par les ingénieurs de Cellebrite. D'autres peuvent être achetées sur internet pour des sommes allant quelques dizaines de milliers à plusieurs millions d'euros, ce qui n'est pas grand chose pour ce genre d'entreprise.

L'entreprise promet plein de choses avec cet appareil, notamment le contournement du code de déverrouillage d'écran sur la plupart des téléphones (donc quand le tel est allumé). Elle promet aussi le déchiffrement de nombreux téléphones, en particulier ceux de la marque Samsung. Cependant leur communication est très marketing, et il semble que nombre de leurs promesses ne soient pas réellement applicables. De plus il n'y a pas forcément la dernière mise à jour d'UFED installée chez les keufs.

13 Voir l'article de mai 2021 « Du nouveau sur l'obligation de donner son code de téléphone en garde-à-vue : comment éviter le traquenard » https://paris-luttes.info/du-nouveau-sur-l-obligation-de-15018 trouvable en format brochure sur https://rajcollective.noblogs.org/materiaux-a-diffuser/

14 https://cellebrite.com/fr/mises-a-jour-des-produits/

communauté de scruter son fonctionnement et avec un peu de chance de reprendre le développement si l'équipe d'origine quitte.
* Une appli non-libre* pourrait volontairement chercher à nuire (de manière large ou de manière ciblée), sans qu'on puisse s'en apercevoir sans l'installer, car sa recette n'est pas rendue publique. Exemples: Skype, malwares et ransomwares cachés dans des jeux, etc.

/!\ Attention, libre* ≠ sécure, une appli libre* peut contenir du code malveillant (volontairement ou non).
De plus, certaines applications ont une réputation, basée sur plusieurs éléments:
* la qualité de l'application dans le temps
* la réactivité à la correction des vulnérabilités
* la réputation de l'équipe de développement
* le modèle économique
* les phénomènes de mode
Enfin, il est important de bien toujours mettre à jour ses applis, afin de profiter des corrections de sécurité.

Voyons quelques applications, pas toutes fiables pareil, pas toutes mises à jour régulièrement, mais toutes libres*.

Magasin d'applications

- F-Droid : propose des applis principalement libres. Attention tout ce qui est dans F-Droid n'est pas forcément extraordinaire: il peut y avoir des pisteurs dans les applications (mais dans ce cas là on peut le savoir), des bouts d'applis qui ne sont pas libres ou encore des failles de sécurité connues, etc. Une partie de ces applis contre indiquées sont recensés sur le site de F-droid dans leur liste "d'antifonction": https://f-droid.org/fr/docs/Anti-Features/
- Aurora Store (interface libre à Google Play Store, permettant de l'utiliser sans compte google) (rappel : les applis dans le Play Store sont pour la plupart non-libres et peuvent potentiellement être modifiées par google). Lorsqu'il y a à la fois aurora store et le google Play Store d'installer, les mises à jours des applis peuvent être faites par défaut par le play store, même si installé par aurora store, ça vaut le coup de désactiver le play store si aurora store a été installé.

Messageries instantannées visant à protéger la confidentialité des communications

- Signal (protocole de chiffrement Signal, compte relié à un numéro de téléphone) (voir nos recommandations de paramètres)
- Briar (protocole de chiffrement Briar, compte pas relié à un téléphone, utilise Tor si on veut, fonctionne aussi sans internet (via Bluetooth)
- Conversations (protocole de chiffrement XMPP/Jabber, d'origine pour ordi, l'appli Android est finalement carrément mieux que ses équivalents ordi)
- Element (protocole de chiffrement Matrix)

Quelques habitudes à mettre en place si ça nous paraît cohérent:
* Se demander à chaque fois comment faire sans téléphone, si possible (aka « Laisser le tel à la maison »)
* Rendre habituel certains usages inhabituels, comme le mode avion par exemple
* Stocker le moins de choses possible sur le tel (documents, photos, contacts, messages). Penser à transférer les photos et fichiers, les transverser dans un ordi de confiance, ou sur un support usb chiffré*.
* Faire de la veille politique et technologique, se former soit même ou avoir un collectif qui se forme. Les téléphones évoluent très rapidement !
* Se former collectivement en cas de garde à vue : bd « je n'ai rien à déclarer » sur https://infokiosques.net, ou « manuel de survie en garde à vue », livre « comment la police interroge et comment s'en défendre » sur https://projet-evasions.org/
* Avoir des téléphones différents pour des usages différents. Avoir un téléphone professionnel, un téléphone pour la militance que je n'allume pas chez moi de préférence. Complexe à appliquer mais intéressant. Il est aussi possible ça soit pris en charge collectivement : que le collectif fournisse des téléphones anonymes pour une tache spécifiques dans la lutte.
* La NSA a dit "redémarre ton tel une fois par semaine". Si il y a une faille exploitée mais pas inscrite dans le téléphone, en redémarrant la faille ne sera plus là.
* Ne pas avoir de téléphone :)

2) Applis libres 📱

Attention ces informations datent de début 2025 et peuvent évoluer particulièrement vite !

Comme on l'a vu, les applications ont un grand pouvoir de surveillance. C'est pourquoi on peut choisir d'utiliser des applications « de confiance ».
Mais alors il faut définir ce que « confiance » signifie, et comment acquérir cette confiance.
La confiance en une appli peut se jouer à différents endroits:
* sécurité "l'appli fait-elle bien ce qu'elle dit et dit-elle bien ce qu'elle fait"
* fiabilité dans le temps : Est-ce que les gens continuent de travailler dessus pour corriger les vulnérabilités ?
* Vérifier réputation des gens qui font le logiciel.
* Tchéquer le modèle économique du logiciel.

Une tendance lorsqu'on parle de sécurité est d'utiliser des logiciels libres*. Pourquoi?
* Avec une appli privative, on ne pourra pas vérifier profondément la qualité de l'appli en terme de sécurité ; et les développeureuses peuvent décider d'arrêter le développement de l'appli sans préavis. Une appli libre* permettra à une

Ce qui est sûr c'est que l'UFED peut contourner les codes de déverrouillage des téléphones <u>non-chiffrés*</u> ou des téléphones <u>chiffrés* mais allumés</u> et cloner la carte SIM.

Le tableau ci-après montre des exemples d'informations susceptibles d'être collectées dans différents matériels de téléphonie :

Téléphone portable	Smartphone (iPhone, Android…)	Tablette (iPad, Android…)
- Liste de contacts - Messages GSM (SMS) - Journal d'appels - Calendrier - Notes personnelles - Photographies …	- Liste de contacts - Messages GSM (SMS-MMS) - Messageries Internet (WhatsApp, Skype, Facebook Messenger, Telegram, SnapChat, Signal…). - Journal d'appels - Photographies - Vidéos - Géolocalisation - Traces de navigation Internet - Agendas - Notes personnelles - Documents - Messagerie électronique …	- Liste de contacts - Messageries Internet (WhatsApp, Skype, Messenger, Telegram, SnapChat…). - Photographies - Vidéos - Géolocalisation - Traces de navigation Internet - Documents - Agendas - Notes personnelles - Messagerie électronique …

IMSI-catcher – les fausses antennes relais [📞]

Il s'agit d'un dispositif se faisant passer pour une antenne relai officielle, qui capte toutes les connexions téléphoniques dans un rayon défini. Il peut être embarqué dans un véhicule. Sa première fonction est de lister les appareils téléphoniques alentours. Il peut aussi intercepter les contenus en clair* tels que les appel et les SMS (en faisant basculer la communication du téléphone sur de la 2G), mais sert principalement à récupérer les métadonnées* : quel téléphone « borne » (est présent dans le rayon défini), quel téléphone appelle quel autre téléphone à quel moment, etc.



La police récupère les numéros IMSI et IMEI et peuvent faire des réquisitions auprès des opérateurs pour savoir à qui ça appartient. Il peut aussi voir les sites internet qu'on fréquente (mais le https protège ce qui est fait sur les sites que l'on visite, lorsqu'il fonctionne). Un IMSI-catcher ne permet pas de prendre le contrôle d'un téléphone ni d'en extraire les données à distance. Le prix d'un IMSI-catcher de qualité pro est d'environ 2000 euros. Pour 50 euros on pourrait s'en fabriquer un, il aura un faible rayon d'efficacité et on devra trouver les outils

permettant de déchiffrer les communications, mais on pourra facilement voir les IMEI alentours et autres infos. Il est aussi possible d'installer un IMSI catcher sur un drone[15].

Perquisition à domicile [📞]

Il y a plusieurs cadres juridique à une perquisition, donc quand ça arrive ça peut valoir le coup de demander dans quel cadre on est (enquête préliminaire, flagrance, instruction). Si c'est une enquête préliminaire, on peut parfois refuser la perquisition, ce que les flics ne vont pas préciser. Nous n'allons pas approfondir cette partie, mais il existe un guide appelé « Se préparer aux perquisitions » disponible ici : https://rajcollective.noblogs.org/materiaux-a-diffuser/. Ce qui n'a pas été mis à jour dans ce guide, c'est que depuis quelques années il est possible d'avoir la présence d'un·e avocat·e lors d'une perquisition (cependant le temps qu'iel arrive ne suspend pas la perquisition).

Boites noires 📱

Les boites noires sont des équipements de surveillance algorithmique qui se développent progressivement et servent aux renseignements (Direction Générale de la Sécurité Intérieure). Ces algorithmes se développent aussi bien pour la téléphonie que pour le numérique. Elles font de la surveillance de masse de la population et émettent des signalement, ainsi en 2020 elles ont effectuées 1739 alertes de personnes à « comportement suspect »[16].

Globalement elles servent à choper la liste des sites internets qu'on visite. Les boites noires font du traitement automatisé de données. Leur réel fonctionnement reste flou, mais elles ne peuvent pas savoir précisément quelles pages on visite lorsque le site est en https (avec le s[écurisé] à la fin – la plupart des sites internets). Couplé à d'autres méthodes de surveillance, ça peut permettre de faire des graphes de profilage.

Équipes technologiques de la police [📞]

Tout au long de ce texte on parle de flics ou de keufs, mais en réalité il existe beaucoup de corps différents au sein de la police et de la justice, qui ont des moyens différents en termes techniques.

La plupart des corps techniques doivent extraire les infos du téléphone sans dégrader celui ci ni laisser de trace de l'intrusion dans le téléphone, c'est ce qu'on appelle « l'analyse forensique ».

15 Exemple sur ce site : https://innovadrone.com/drone-imsi-catcher/
16 https://www.nextinpact.com/article/69817/6-000-comptes-informatiques-sont-connectes-aux-grandes-oreilles-renseignement

IV) Réduction des risques

/!\ Attention ce chapitre évolue particulièrement vite dans le temps. Se renseigner sur l'évolution au cours du temps.

Vous pouvez retrouver cette partie sur le wiki https://telmob.0id.org/. Il s'agit d'un wiki donc il est possible de contribuer / modifier.

La sécurité absolu pour les téléphones est impossible, ce que l'on veut c'est réduire les risques de vols de données.

Ce qui est important c'est de réfléchir / comprendre les menaces qui s'appliquent à nous individuellement et collectivement. Pour réduire les risques, avoir plus de contrôle de ses communications, plusieurs outils sont à notre disposition.

On peut classer ces outils en quelques catégories:

- habitudes, manières d'utiliser le téléphone, questionner les usages

- choix d'applications

- paramètres du téléphone

- avoir un téléphone « anonyme »

- les trucs de geekos (technique)

1) Habitudes [📞]

Le plan des habitudes est le plus important, car comme on l'a vu, utiliser des téléphones portables implique un grand nombre de problèmes inévitables.
* La première habitude à prendre consiste à se poser les bonnes questions. La « modélisation de la menace » est un outil nous permettant de choisir des réponses adaptées à nos besoins. C'est un outil à expérimenter et utiliser individuellement et collectivement car nos choix auront des conséquences sur notre entourage.
→ Qui sont nos ennemi·e·s potentiel·le·s? (flics en garde à vue, agent de renseignement derrière son ordi, agent en filature, fachos, voisin.nes, cohabitant.es…)
→ Que veut-on leur cacher? (liste de contacts, membres d'un groupe signal, contenu de message, localisation, sites web visités, documents enregistrés…)
→ Que risquons-nous si on échoue? (se faire gronder, perdre nos données, prendre une amende, aller en prison…)
→ Quels moyens nos ennemi.es sont-iels prêt.es à mettre pour nous ou nos activités? (respect de la loi ou pas, quantité d'argent disponible, protection légale…)
→ Quelle énergie avons-nous à mettre pour nous protéger?

accès à l’appareil, ou logiciel en installant à distance ou à partir de l’appareil des logiciels malveillants.

Un des logiciels très médiatisé faisant cela est **Pegasus** qui permet de fouiller dans les données (calendriers, photos, contacts, messageries, appels enregistrés, coordonnées GPS…) des smartphones, iPhone comme Android, infectés, mais aussi de contrôler à distance la caméra et le micro intégrés à l’appareil, ce qui donne entre autres la possibilité d’écouter des conversations dans une pièce alors que le téléphone apparaît inactif. Un outil avait été développé en 2021 pour essayer de détecter sa présence dans son téléphone mais nécessitant des compétences informatiques[20]. En 2021 pegasus pouvait être installé sur un téléphone en faisant cliqué sur un lien ou via une faille de sécurité de Whatsapp, la victime recevait ce qui ressemble à un appel vidéo qui suffit à infecter le téléphone dès la première sonnerie, même si elle ne répond pas. A priori la France n’utilise pas ce logiciel dont le coup d’acquisition pour une structure est à quelques dizaines de millions d’euros.

Voici quelques noms générales de logiciels malveillants si envie de voir leur capacité : PlainGnome, BoneSpy, Monokle, NoviSpy, Mandrake, AwSpy, … Ils ne sont pas forcément utilisés par les renseignements français.

A savoir en plus des prix des logiciels il y a des enjeux géopolitiques autour des logiciels utilisés ce qui peut expliquer le fait qu’ils ne sont pas utilisés partout. En fonction de quelle entreprise ou pays propose le système de surveillance, les utiliser dans le renseignement français c’est donner des accès à ce qui intéresse les renseignements à ces structures.

20 Mobile Verification Toolkit : https://github.com/mvt-project/mvt

Type de parcours possible lors d’une enquête : Il existe une cellule qui travaille sur une instruction, celle-ci envoie au département informatique-électronique l'IRCGN (Institut de Recherche Criminelle de la Gendarmerie Nationale) qui a pour mission d’extraire le contenu d’un téléphone et de le ranger dans un disque dur. Celui-ci peut aussi se déplacer et être présent lors de perquisitions. Si cette institution est bloquée par un support chiffré elle peut décider de l’envoyer au CTA (centre technique assistance). Si des informations sont extraites elles sont renvoyées à la cellule d’enquête.



- L’ **Institut de Recherche Criminelle de la Gendarmerie Nationale** qui a un statut militaire au sein duquel se trouve le Département informatique-électronique (INL). « *Ce dernier traite de la preuve numérique sur tous types de supports, en particulier sur les disques durs et les téléphones portables. Assurant des expertises judiciaires et des examens scientifiques au profit des magistrats et des enquêteurs, il est également en mesure de les assister sur le terrain ou à distance, lors de perquisitions ou d’auditions en milieu complexe.* » Il dispose d’enquêteur en technologies numériques (N-Tech), qui sont gendarmes, avec une formation d’officiers de police ainsi qu’une formation dans le domaine informatique de 15 mois à l’UTT de Troyes.



- **Le Centre Technique d’Assistance** : « *[...] l’Etat s’est doté dès 2001 d’un organisme à vocation interministérielle, le Centre Technique d’Assistance (CTA) rattaché au ministère de l’Intérieur et aujourd’hui placé sous l’autorité de la DGSI. Il est au service des magistrats et des enquêteurs qui le sollicitent et constitue un niveau d’intervention technique supérieur mis à leur disposition pour augmenter les chances de succès de leurs investigations lorsque les délinquants et criminels ont fait usage de moyens de chiffrement.* » . Le CTA est couvert par le secret défense et a le droit d’utiliser des techniques pouvant détruire le matériel à étudier.



L'IRCGN peut être remplacé par des entreprises d'ingénieur.es agrées sous traitante comme par exemple :



- Tracip : https://www.tracip.fr/
- Informatique legal https://informatique-legale.com/
- Laboratoire évidences SAS : https://evidences-lab.com/

Plus d'informations sur les équipes techniques:

- "Blog d'un informaticien ancien expert judiciaire" : https://zythom.fr/

- "the french intelligence", compilation de textes sur les renseignements français: https://infokiosques.net/spip.php?article1821

Exploitation de failles de sécurité 📱

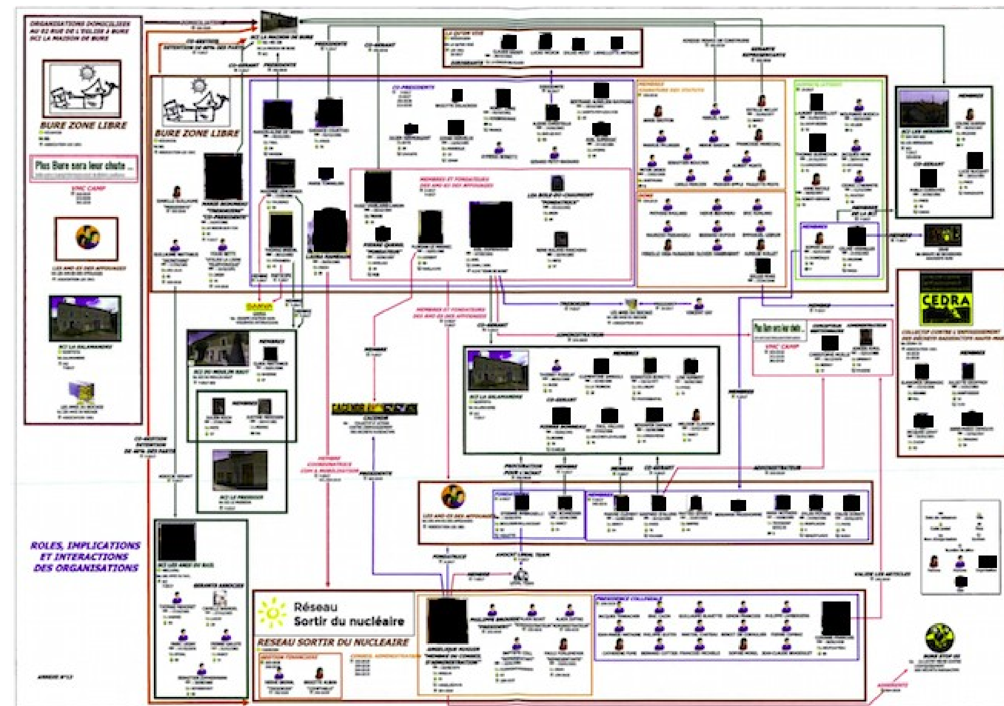
Il semble que c'est plutôt pratiqué par le Centre Technique d'Assistance (CTA). Par exemple le CTA peut arriver à extraire certaines informations des Iphones 5 à X chiffré (des images ou des informations de géolocalisation de certaines applications, des infortions de connection à des réseaux Wifi ou Bluetooth… [17]

Analyst's Notebook et logiciels d'analyse de données [📞]

Logiciel proposé par I2, sous groupe d'IBM, le géant des microprocesseur. Il est utilisé par le Service central de renseignement criminel sous le nom ANACRIM pour analyste criminel (dont on confond souvent le nom de l'équipe de gendarmerie avec celui du logiciel).

Outil d'analyse des flics qui leur permet de faire des graphes de qui parle avec qui, ils injectent dans le logiciel toutes les informations récoltés principalement dans les communications téléphoniques (que ce soit sur les personnes, lieux, évènements, le matériel). Ainsi dans les enquêtes sur des militant-es, ils essayent de mettre en avant des « organisateur.ices » de tel mouvement qui est en contact avec beaucoup de personnes militantes, ou des personnes qui font liens entre plusieurs univers.

17 Si envie d'avoir plus d'informations techniques à ce sujet il s'agit de la méthode « BFU » (Before First Unlock) https://blog.elcomsoft.com/2019/12/bfu-extraction-forensic-analysis-of-locked-and-disabled-iphones/



Exemple de graphe fait par le logiciel Analyst's Notebook sur une enquête à Bure.[18] *Ce graphe basé sur les communications entre les gens permet de ranger chaque personne dans des rôles supposés vis à vis de la lutte.*

Tentative de restauration des données à partir d'appareils endommagés [📞]

On n'a pas d'éléments d'usage à ce sujet, mais il existe des corps de polices qui essayent de récupérer des données de supports numériques cassés ou partiellement brûlé[19]. Ces techniques semblent être utilisés dans des affaires plus importantes.

Installation de mouchards (matériel ou logiciel) [📞]

C'est possible que ça soit fait dans le cadre du renseignement. Par exemple l'installation d'un mouchard qui surveille ce qui se passe sur les autres applications, allumer les micros à distance, activer et transmettre la géolocalisation, feindre quele téléphone est éteind. Les mouchards peuvent être matériel, ce qui nécessite d'avoir

18 Information disponible sur l'article https://reporterre.net/La-justice-a-massivement-surveille-les-militants-antinucleaires-de-Bure qui développe les outils de surveillance utilisés dans le cadre de l'instruction pour association de malfaiteur à Bure, dont beaucoup sur la téléphonie.

19 https://www.nextinpact.com/article/29762/108071-la-nouvelle-arme-anti-cryptographie-gendarmerie